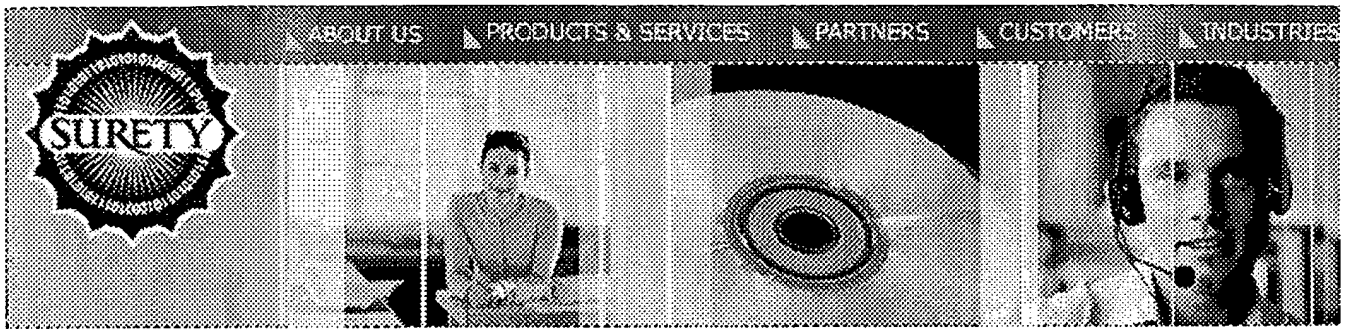
Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	93402	transcript$	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 10:21
S2	3863	transcript$ & signature	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/11 16:10
S3	4	(transcript$ & signature) & "electronic transcript"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 15:40
S4	133	RIPEMD$	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 10:21
S5	105	RIPEMD-160	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 10:21
S6	0	RIPEMD-160 & has	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 10:21
S7	104	RIPEMD-160 & hash	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 10:21
S8	11	RIPEMD-160 & transcript$	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 10:22
S9	11	(RIPEMD-160 & transcript$) & hash	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2004/06/14 10:22
S10	118063	transcript$	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22
S11	5324	transcript$ & signature	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22
S12	8	(transcript$ & signature) & "electronic transcript"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22

S13	258	RIPEMD$	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22
S14	203	RIPEMD-160	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22
S15	0	RIPEMD-160 & has	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22
S16	202	RIPEMD-160 & hash	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22
S18	12	(RIPEMD-160 & transcript$) & hash	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:22
S19	12	RIPEMD-160 & transcript$	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:35
S20	23	"electronic transcript"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:39
S21	50	"e transcript"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:44
S22	106	"digital notary"	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2005/09/16 13:44
S23	22	surety.as.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2005/09/16 15:04
S24	4	S23 & hash$	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2005/09/16 14:13
S25	2	"5136647".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2005/09/16 15:05

S26	10	("5136647" "5136646" "5373561" "4309569" "5781629").pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2005/09/16 15:07
S27	28	("5781629").URPN.	USPAT	OR	OFF	2005/09/16 15:22



Products + Services

Surety's Products and Services are designed to meet the needs of the **Small Business** as well as those of the **Large Enterprise**. With AbsoluteProof®, you can irrefutably prove that your electronic records have never been altered, far into the future.

Whether you subscribe to our service or license our software and run it yourself, you receive the same level of electronic record integrity assurances. Surety's Professional Services team is available, should you need help integrating AbsoluteProof into your business processes.

Our offerings include:

- **ABSOLUTEPROOF SERVICE.** AbsoluteProof is a third-party digital time-stamping service used by customers worldwide to independently prove the authenticity and integrity of their vital electronic records, now and at any time in the future
- **ABSOLUTEPROOF ENTERPRISE.** For enterprises that wish to run the AbsoluteProof Service inside their network, an AbsoluteProof software license is available for purchase.
- **PROFESSIONAL SERVICES.** Surety backs all of its products with a dedicated and seasoned professional services team—standing ready to help you seamlessly integrate AbsoluteProof into your environment.

These offerings can be combined in various ways to meet the unique needs of your business. Contact Surety Sales for additional information.

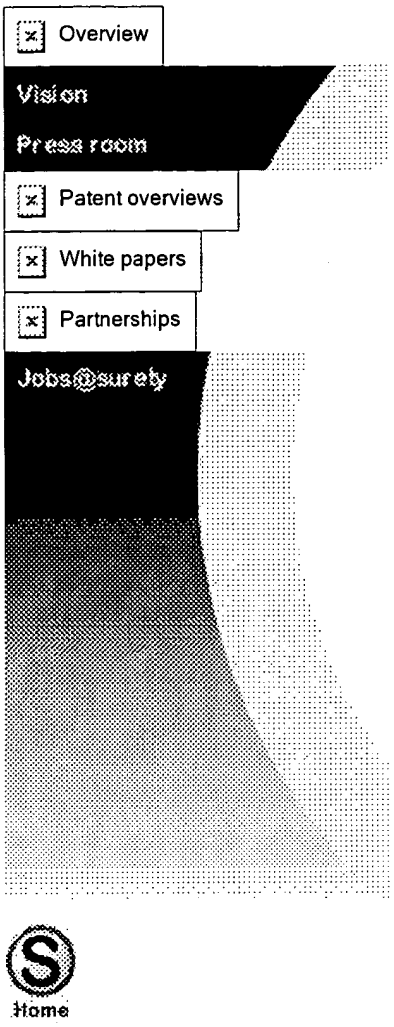
CONTACT U

800.298.3115
703.707.9910
info@surety.com

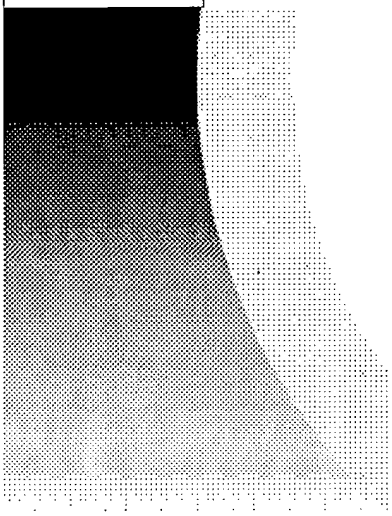
NEWS & EVENT

HOW IT WORK
THE BENEFIT
DEPLOYMENT OPTION

 © 2005, Surety, LLC All rights reserved.


Overview
Vision
Press room
Patent overviews
White papers
Partnerships
Jobs@surety
Home

- Overview
- Vision
- Press room
- Patent overviews
- White papers
- Partnerships
- Jobs@Surety



Home

e-transcript hash Homepage | Advanced Search

Search using: Ask Jeeves Google

CUSTOM WEB FILTERS HotBot Skins | Prefe

Date: **Before June 6 2000** [Edit this Search]

Sorry, your search had no web results

Revise your search query and try these tips:

- Check your spelling.
- Try using fewer words, or more general terms.
- Use fewer filters for your search.
- Use Search Tips to improve your search results.

Search for "**e-transcript hash**" using: Google

Advertise | Help | Text-only Skin | Submit Site | HotBot International | Yellow Pages
© Copyright 2005, Lycos, Inc. All Rights Reserved. | **Privacy Policy** | Terms & Conditions | **HotBot Your Site**

e-transcript hash Homepage | Advanced Search

Search using: Ask Jeeves Google

CUSTOM WEB FILTERS HotBot Skins | Prefe

Date: **Before June 6 2000** [Edit this Search]

SPONSORED LINKS (filters not applied)

- Protext Free Downloads
 Better condensed transcripts and keyword indexes - all at less cost
 www.protext.com

- ES Deposition Management
 Worldwide Deposition Services Accurate, timely, & professional!
 www.eastwood-stein.com

WEB RESULTS by Jeeves (Showing Results 1 - 10 of 257)

1. McGinnis & Associates: PubNETics **e-transcript**
PubNETics **e-transcript** T McGinnis & Associates, Inc. Offers Secure and Accurate Transcripts D instantly by **e**-mail
www.mcginniscourtreporters.com/pubnetics.html

2. **transcript**-engfin.PDF
SEMINAR ON LABOUR LEGISLATION IN CHILE CANADA-CHILE AGREEMENT ON LABOUR COOPE OTTAWA APRIL 30, 1998WARREN EDMONDSON: Good morning.
www110.hrdc-drhc.gc.ca/pdf/pdf_e/transcript-engfin.pdf

3. etranscript
...for electronic **transcript** delivery. The only electronic **transcript** delivery product endorsed b Service Corporation, **e-transcript** lets...
www.prosystemsweb.com/etranscr.htm

4. **E**-Transcripts
E-Transcript alleviates formatting problems: Electronic and paper transcripts maintain identica line integrity. The **E-Transcript**...
www.simpsonreporters.com/E-Transcripts/e-transcripts.html

5. Litigation Technology Resources - NetTech, Inc.
Bowne's JFS Litigator's Notebook. Concordance. **E-Transcript** Binder. MeltingPoint. Summatior Transcription. CaseViewII. ...
www.nettechinc.com/littech.htm

6. "Streaming over a collection" | coll str | self halt.
...str do: [:**e** | **Transcript** nextPut: **e**]. **Transcript** flush.
www.coling.uni-freiburg.de/~sue/smalltalk/streams.st

7. Fenichel's CURRENT TOPICS IN PSYCHOLOGY
Alphabetical Pointer: A | B | C | D | **E** | F | G | H | I | J-K | L | M | N | O ... Suler) Healthy and Internet Use **Transcript**: Live...
www.fenichel.com/Current.shtml

8. courtopinions
...full text can be ordered by **e**-mail.) Florida, Middle District, www.flmd.uscourts.gov... www.nlj.com/special/courts.shtml

9. Drosophila CtBP: a Hairy-interacting protein required for...
4C). The maternal **transcript** persists throughout the early embryonic stages (Figure 4D and **E** levels drop during gastrulation and...
embojournal.npgjournals.com/cgi/content/full/17/7/2067

10. Sterol Carrier Protein-2 Overexpression Enhances Sterol Cycling...
Apurba K. Gayen , Margaret **E**. Groh and Kevin Schadick ... Apolipoprotein **transcript** abundan determined in total RNA extracted as described...
www.jbc.org/cgi/content/full/272/10/6490

« Previous | Next »

Search for "**e-transcript**" using: Google

Advertise | Help | Text-only Skin | Submit Site | HotBot International | Yellow Pages
© Copyright 2005, Lycos, Inc. All Rights Reserved. | **Privacy Policy** | Terms & Conditions | **HotBot Your Site**



Legal guide

Guide for Legal Counsel on mitigation of risk from electronic records [1]

By Charles R. Merrill, Esq.[2]
June 22, 1995

With the Information Age already beyond infancy, there is no longer any doubt about the advantages of using digital computers to store, access, and communicate information in magnetic, electronic, or optical formats, collectively referred to here as "electronic records."

Prodigious space and cost savings, the ability to sort and search, the ability to edit, and the capability for instant transmission anywhere on the Net are only some of the well-known advantages of electronic records over paper records. When faced with the opportunity to convert paper records to digital format, the question is a "no-brainer" for most managers.

Yet, the reality is that the Information Age is still awkwardly immature. The technology has far outpaced the ability of management and security systems to keep

the technology under prudent control. Sage and settled legal principles in this capricious environment have not yet developed sufficiently to predict how responsibility for the risks and damages of unruly or unexpected behavior are to be allocated among active and passive innocent victims.

The promise of the paperless society (or at least one with significantly less paper) is unlikely to be fully realized until risk managers (including legal counsel and other consultants) of the corporate and commercial arena signal a working consensus that the risks inherent in electronic records are under control and are justified by their advantages.

This paper will serve to introduce you to a system that, from your perspective as legal counsel, serves to control or mitigate precisely these risks. It explains how the patented[3] technology of the Digital Notary Record Authentication System[4] holds the promise of a major breakthrough in security services for electronic records.

As will be explained below, the Digital Notary Record Authentication System equips your enterprise to routinely freeze the content of your electronic records in time, so that both their content and time-date stamp are reliably authenticated and non-repudiatable, even in the challenging environment of an open insecure system such as the Internet. Moreover, unlike the typical public key cryptosystem, the Digital Notary Record Authentication System does not require the maintenance and protection of any public or private encryption "keys," and thus provides a dimension of security which is independent of any compromise of such keys.

Accordingly, the Digital Notary Record Authentication System is uniquely positioned not only to enhance and complement many of the authentication services furnished by public key cryptographic technologies and protocols, but to offer an entirely new domain of high value services that unequivocally detect tampering, backdating, or deterioration in electronic records. The result is stronger security for your enterprise and its data.

Footnotes for above:

(1) This paper is intended for the use of legal counsel and other risk managers in spotting points of vulnerability in electronic record systems which can perhaps be cured or mitigated by the Digital Notary Record Authentication System. This paper is intended as general information rather than as legal advice applicable to any particular situation, entity, or jurisdiction, and does not create any attorney-client relationship. Nor does it create any warranty enforceable by anyone.

(2) Mr. Merrill (5338481@mcimail.com) is a partner of the law firm of McCarter & English in Newark, NJ (with offices in Cherry Hill NJ, Wilmington DE, New York NY, and Boca Raton FL), where he chairs the firm's Computer and High Technology Law Practice Group. Merrill is an active member of the Information Security Committee of the American Bar Association Section of Science and Technology, currently formulating rules and guidelines for public key certification authorities. A frequent speaker and writer in different areas of information law, he currently serves as national moderator of the Lexis Counsel Connect online forum, E-Mail and Electronic Commerce, and as Online Editor of *The DataLaw Report*, published by Clark Boardman Callaghan, and is a trustee of the Venture Association of New Jersey. Merrill received an LL.B. from Harvard Law School, an A.B. With Honors (in Political Economy) from Williams College, and an LL.M. (in Taxation) from New York University Law School, and is a member of Phi Beta Kappa. He is a member of the New Jersey Bar and the U.S. Tax Court. The views expressed in this paper are Mr. Merrill's own, and do not necessarily reflect those of any organizations with which he

is affiliated.

(3) U.S. Patent Nos. 5,136,646, 5,136,647 (8/4/92) and 5,373,561 (12/13/94), Stuart A. Haber and Wakefield S. Stornetta, Jr., inventors., and portions of U.S. Patent No. 4,309,569.

(4) For information, contact Surety, Inc., 1890 Preston White Drive, Reston, VA 20191, 703.264.8818 (voice), 703.264.2788 (fax), or info@surety.com on the Internet, or http://web.archive.org/web/20020206203447/http://www.surety.com/ on the World Wide Web.

Legal Problems of Electronic Records

A. In General

Some of the legal problems with electronic records are not completely based on rational analysis, and stem simply from the fact of the information age's relative immaturity. The inner workings of computer hardware and software systems are only now becoming part of general education and awareness, and are still novel and mysterious to most people.

Electronic records contained on various electronic storage media, such as floppy diskette, PC hard drive, tape, and CD-ROM do not have the familiar and tangible look and feel of traditional books of record displayed in inked, pencilled, typed, or printed paper records. As you might expect, electronic records are not intuitively well understood by witnesses, judges, and juries. A fair amount of legal confusion has been the result ever since the legal system began trying to force electronic records into legal pigeonholes developed to govern paper records.

It is a fact of life that commercial techniques and customs tend to adapt slowly to changes in technology. It tends to take even longer for novel implications to be experienced and analyzed sufficiently to foster the development of practical legal principles which are truly responsive to reality.

In the case of electronic records, the galloping pace of change through the last few decades has resulted in two opposite extremes of overreaction by the legal system. Whereas electronic records initially were mistrusted by a conservative legal system because novel computer technology was poorly understood, we have come full circle. Having persuaded the courts to embrace electronic records enthusiastically because of their convenience and flexibility, today we are experiencing an overreaction toward a progressive judicial attitude of unwarranted trust in the reliability of unprotected electronic records.

As we will see below in the discussion of admissibility and probative value of electronic records in evidence, the legal system is again failing to keep pace with technology. The cosmic tension between parallel advances in the art of attacking electronic records, and the art of protecting electronic records from attack is not yet widely understood or appreciated. When sporadic and inconsistent judicial decisions begin to support successful attacks on the credibility of unprotected electronic records, the aftershocks may well undermine the credibility of all existing naked electronic records. The Digital Notary Record Authentication System can mitigate the risk of such uncertainty.

B. Enforceability Under Statute of Frauds - The Good News

The good news in this legal guided tour is that the outdated Statute of Frauds - originally designed for a paradigm shift to a society based on paper in the sixteenth century - appears unlikely to further obstruct the paradigm shift away from a paper society at the dawn of the twenty-first century.

The Statute of Frauds, as embodied in the Uniform Commercial Code[5] requires an enforceable contract to be in "writing" which is "signed" by the party against whom enforcement is sought. "Writing" is defined by §1-201(46) to include "...[P]rinting, typewriting or any other intentional reduction to tangible form." "Signed" is defined by §1-201(39) as "[A]ny symbol executed or adopted by a party with present intention to authenticate a writing.

After some early difficulty with considering magnetic and electronic phenomena to be a "reduction to tangible form," it is a fair summary that most jurisdictions today consider an electronic record to be a "writing" for Statute of Fraud purposes,[6] particularly if the electronic record is capable of being printed onto hardcopy. Similarly, although "authenticate" in the electronic context is not usefully defined in the U.C.C.[7] , electronic records such as e-mail or fax communications which evidence directly or circumstantially the sender's assent and self-identification, have generally come to be considered "signed writings" for purposes of the Statute of Frauds.[8]

The bar to enforceability under the Statute of Frauds has always been subject to many exceptions,[9] and opinion is strongly building in favor of repealing the Statute of Frauds for the sale of goods and other purposes.[10] The good news, therefore, is that electronic records are today fairly unlikely to be held unenforceable under the Statute of Frauds.

Footnotes for above:

(5)U.C.C. §2-201(1) Governing Sale of Goods: "Except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker." (emphasis added). See also U.C.C. §5-104(1) governing letters of credit; U.C.C. §8-319 governing sale of securities; U.C.C. §9-203 governing security interests; U.C.C. §1-206 governing contracts for the sale of other kinds of personal property over $5000.

(6) There are cases involving special statutory "writing" requirements where an electronic record would not suffice because of particular policy requirements. See, e.g., *Common Carrier Motor Freight Assn. v. NCH Corp.* 788 S.W.2d 207 (Tex Ct.App.1990)

(7) See Baum, "Linking Security and the Law of Computer-Based Commerce", p. 4, *Workshop on Security Procedures for the Interchange of Electronic Documents* (NIST Abridged Version NISTR 5247, 1994), reprinted in Prentice Hall Law and Business, Current Developments in Computer Litigation (Seminar Materials, Sept 1994).

(8) See generally, Wright, *The Law of Electronic Commerce* Chapter 16 (1991

and annual supplements through 1994).

(9) For example, between merchants under U.C.C. §2-201(2).

(10) See recommendations of Article 2 Study Committee and August 1994 Draft Revisions of the Drafting Committee of the National Conference of Commissioners on Uniform State Laws and the American Law Institute (August 1994 draft not yet finalized). Also, in August, the Commissioners gave approval to a new Article 8 on Investment Securities which eliminates the Statute of Frauds writing requirement from that statute. E-mail correspondence with Prof. Amelia G. Boss, December 6, 1994. In October of 1994, the State of New York effectively abolished the Statute of Frauds applicable to a "qualified financial contract" (contracts for currency, commodities, options and the like) by considering "tangible written text produced by computer retrieval" as satisfying the requirement of a writing, and by considering "any symbol executed or adopted by a party with the present intention to authenticate a writing" as constituting a signing.

C. Admissibility of Evidence

Although there are other avenues, the principal theory for admissibility of business records - both paper and electronic records - is the "business records exception" to the hearsay rule[11] provided by Federal Rules of Evidence (hereinafter "FRE") 803(6), and under various similar State statutes, providing:

> "A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness. The term 'business' as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit."

The justification for the business records exception harks back to the day of a company's single-copy leatherbound pen-and-ink shop books. These books were considered trustworthy because the company relied upon them in daily business, and the opposing party had an opportunity to detect alterations and deletions in the sewn-in pages. The business records exception is also supported by the doctrine of necessity. The introduction of the shop books into evidence avoids the need to have many different company employees testify.[12]

It is important to note that the business exception rule generally allows the statement into evidence unless the opposing party carries the burden of showing lack of trustworthiness. In his pioneering 1986 law review article,[13]

Professor Rudolph Peritz observes that the burden of opposing even untrustworthy electronic evidence is an onerous one. Arguing for electronic records to be governed by a tighter standard of admissibility, Prof. Peritz observes disapprovingly that an offer of computerized business records (if not specially prepared for trial) is rarely turned down by the trial court, even in cases where the presumption of trustworthiness is shown to be unjustified[14].

> "The presumption of trustworthiness simply carries too much weight in our recently computerized society. Judges, juries, attorneys and parties cannot make sound judgments regarding the credibility of computerized records by comparing fairly brief and understandable testimony with recognizable documents, as they could with traditional shop books. Unlike ledgers and books of payables, and receivables with individual items, intermediate accounts, and scrivened entries or changes, computer printouts are not records at all, but rather neatly packaged concatenations of information excerpted from numerous records in multiple files. Because program changes or data manipulations can be accomplished without leaving any trace and without affecting the day-to-day operation of a computer system, both unintentional error and intentional fraud are difficult to discover behind a perfect-looking printout."[15]

Footnotes for above:

(11) Hearsay is a statement made outside the trial, which is offered at trial to prove the truth of the material in the statement. On the theory that the statement is not subject to cross-examination in front of the fact-finder, hearsay is inadmissible in evidence unless an exception applies. See Baum and Perritt, *Electronic Contracting, Publishing, and EDI Law* §6.27 at p. 354 (John Wiley & Sons, Inc. 1991).

(12) Peritz, "Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence," 80 NW Univ Law Rev 956, 957 (1986).

(13) Id., at 958.

(14) Id., at 958.

(15) Id., at 960. See also Baum, at 4, citing Peritz, and quoting *U.S. Dept. of Justice, Admissibility of Electronically Filed Federal Records as Evidence: A Guideline for Federal Managers and Counsel* (Oct 1990) at 2: "[B]ecause electronic files are particularly susceptible to purposeful or accidental alteration, or incorrect processing, laying a foundation for their admission must be done with particular care. Proper control over creation and maintenance of these files can be crucial in overcoming inevitable objections that will be raised in the courtroom."

In his landmark paper, "Linking Security and the Law of Computer-Based Commerce,"[16] Michael Baum joins Professor Peritz in favoring of tightening the foundation requirements for electronic records, and cites with approval authorities[17] tending to lend support for this view. Prof. Peritz cites a number of extremely liberal (i.e., in favor of admissibility) decisions[18] as indications of a trend toward further relaxation of the standard, but Baum disagrees. Instead, Baum persuasively distinguishes these latter cases because in none of them was the proponent of the evidence also the custodian of the electronic evidence. Rather, "... each of these cases involved telephone company billing records – records which are created and retained by trusted third parties."[19] In the absence of a trusted third party as custodian of electronic records, therefore, Baum argues that evidence offered under the business exception rule can and should be excluded if the opponent of the digital evidence makes a strong enough showing of untrustworthiness.

Another hurdle to admissibility is authentication, namely proof that the document is what it purports to be, and that there is a relevant relationship between the document and a particular person, who is frequently a party to the litigation. An example of authentication under traditional principles is proof of a connection between a promissory note and the purported maker, by authenticating the signature on the note. A contemporary example highlighting the particular problems of electronic evidence is the difficulty in authenticating an email message stored on the company's LAN, which purports to be an email message sent by Alice to Bob on June 30, 1994 at noon, containing merely the ASCII characters at the bottom, "Regards, Alice".

Professor Peritz observes disapprovingly that most commentators have come to view the requirement of authentication as too time-consuming and expensive as a condition upon admissibility, because of the common perception that most writings turn out to be genuine, and that the opponent who seeks to avoid the connection to the document is perhaps in the best position to demonstrate fraud or mistake. Peritz doubts, however, whether these reasons are at all persuasive when we are dealing with electronic records. He cogently points out that there is actually no genuine business record, but only a computer printout which is a report of what is stored in the computer. Moreover, it is far more likely that the proponent of such evidence, rather than the opponent, will be in a position to be familiar with the computer system which produced it[20].

One conceptual approach to authentication, either for admissibility or in support of the probative value of the evidence after it is admitted, is FRE 901 (b)(9), which provides that technological evidence is to be supported by "[e] vidence describing a process or system used to produce a result and showing that process or system produces an accurate result." *In The Law of Electronic Commerce* (1991), at 113, Ben Wright cites the Advisory Committee Note to FRE 901(b)(9) for the purpose of this rule:

> ". . .[T]his rule is designed especially for computer business records. Thus, competent testimony identifying, describing the function of, and confirming the accuracy of a computer system that produced a message or record is sufficient to authenticate the message or record. It is not necessary to bring the computer system itself into the courtroom for a demonstration."

Footnotes for above:

(16) Ibid., at 5.

(17) "See *U.S. v. Scholle*, 553 F.2d 1109, 1124-25 (8th Cir.), *cert. denied*, 434 U.S. 940 (1977)(stating that computer storage needs a more comprehensive foundation for admissibility, including testimony on procedures for input control, such as a test for insuring accuracy and reliability); *U.S. v. Russo*, 480 F.2d 1228, 1239-44 (6th Cir. 1973)(holding that the authentication of computer records requires establishing reliability and trustworthiness of information put into computer)." Baum at 5, n. 16

(18) See, e.g., *Rosenburg v. Collins*, 624 F.2d 649 (5th Cir. 1908); *U.S. v. Vela*, 673 F.2d 86, reh'g den., 677 F.2d 113 (5th Cir. 1982), and *U.S. v. Linn*, 880 F.2d 209 (9th Cir. 1989). Baum at 5, n. 17.

(19) Baum, at 5, n. 17. See also Stanley A. Kurzban, "Authentication of Computer-Generated Evidence in the United States Federal Courts," at 8 (unpublished, October 1994), who distinguishes a situation where the case turns on the electronic records, and the party with custody may have sophisticated computer skills in its enterprise: "Courts should be specially concerned about the authenticity of direct, rather than incidental, computer-generated evidence of wrongdoing, whether business records or not. If evidence is germane rather than peripheral to the issues of a case, successful counterfeiting of data may have a greater and more predictable effect on the outcome of a proceeding. In such cases, the defendants may be sophisticated users of computers. They may know how to tamper with computers and may assert, with cause, that others may have fabricated computer-generated evidence to their detriment..."

(20) Peritz, at 978.

All three of the above commentators (Peritz, Baum, and Wright) recognize that courts do not generally tend to require proponents of evidence to satisfy FRE 901(b)(9), and instead tend to rely merely upon the presumption of trustworthiness under the business exception rule FRE 803(6), discussed above. In the case of electronic records, however, there is difference of opinion among commentators: Peritz and Baum argue for requiring a 901(b)(9) showing by the proponent, and Wright argues the reverse[21]. The Advisory Committee's note to FRE 901(b)(9) rather neutrally provides that a court may take judicial notice of the accuracy of a system or process, but cautions that "taking notice of a process's accuracy does not mean taking notice of a particular result as accurate." [22]

The "best evidence rule," FRE 1001(1), generally requires the use of the original of a "writing" or "recording," defined as "letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other forms of data compilation." In the case of computer-produced information, the best evidence rule virtually disappears. FRE 1001(3) defines the original to include printout or other output "readable by sight, shown to reflect the data accurately."[23]

D. Probative Value of Evidence Once Admitted

If evidence is ruled admissible, then the spotlight for testing electronic evidence shifts to arguments as to the probative value of the evidence, which party has the burden of producing evidence, which party has the burden of persuasion before the fact-finder, and whether one party has the right to summary judgment because there are no material facts in dispute.

Dramatic new legal principles are emerging, which (as suggested in the title of the Baum article, supra) directly link the security of electronic records with the law of commerce governing those records. One example is U.C.C. Article 4A, governing wholesale fund transfers, which can shift the loss of an unauthorized order between two innocent parties, depending upon the "commercial reasonableness of a security procedure."[24] Similarly, under the draft model EDI law of the United Nations Commission on International Trade Law (UNCITRAL),

> **"Information presented in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor." UNCITRAL, *Draft Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication* (Working Group, 28th Session Vienna October 3-14, 1994)(as posted by Prof. Amelia G. Boss on Lexis Counsel Connect, Law of the Electronic Road Seminar, Nov 28 1994)**

On March 10, 1995, the State of Utah enacted a Digital Signature Law, based upon a public key cryptosystem supported by a system of certification authorities, the world's first attempt at a comprehensive legislative system for authenticating electronic records (it also provides for time-date stamping) so that electronic records meeting the standards of the bill will become reliably non-repudiatable. As of this writing, bills have been introduced into the State Legislatures of California and Washington State, closely resembling the Utah Digital Signature Law[25].

Footnotes for above:

(21) Wright, *Law of Electronic Commerce*, at 118-9 (1991).

(22) Peritz, at 983.

(23) See Baum and Perritt, §6.26, at 351. Peritz considers "inexplicable" the FRE's treatment of printouts as "originals" and magnetic tape and disk copies as "copies," since printouts are typically created from the data stored on magnetic tapes or disks. Peritz, at 983.

(24) See Baum, at 13, n. 45.

(25) 1995 UT S.B. 82; 1995 CA A.B. 1577; 1995 WA A.B_____.

Wright, Law of Electronic Commerce, at 118-9 (1991).

The Security of Electronic Records

Electronic records, without the right precautions, are notoriously easy to forge and alter with a modest amount of computer skill and access to the record. "But," runs the counter argument, "paper records can also be forged and altered." The answer is that non-detectable forgery or alteration of paper records requires some training, skill, and effort. It is child's play for a mischievous or disgruntled employee with a computer to alter an existing electronic copy of a word-processed document (or substitute a new bogus document) so that the altered or forged record is utterly indistinguishable from the original or true record.

Matters are further exacerbated by the increasing reliance upon email, not only on a protected Local Area Network (LAN) within the enterprise, but also connected to worldwide open systems through Wide Area Network (WAN) gateways. Urgent messages routinely arrive in great volume without any traditional identifying cues, such as the visual cue of a face-to-face talk, the aural cue of a telephone voice, the visual cue of a signature, or the relational cue of the messenger's identity. The result is a greatly expanded potential for undetectable forgery or alteration, as well as elevated exposure to damage from instant and broad dissemination. If the link from one enterprise to another enterprise meanders along unpredictable byways through privately owned hosts on the unregulated Internet, further opportunities for intercepting and surreptitiously altering electronic records are promiscuously spawned.

Attempted Solutions Prior to the Digital Notary Record Authentication System

In response to the increased vulnerability of electronic records, ingenious schemes have been developed to enhance the security of electronic records.

Inside the closed environment of the enterprise, or between two frequent EDI trading partners sharing a common security umbrella, enhanced physical security and more sophisticated log-in protection techniques can significantly advance the security of the enterprise's electronic records. However, since the information flow of the typical enterprise has shifted from the secure glassed-in citadel of the MIS department to a computer on everyone's desk and in everyone's briefcase, it is increasingly difficult for the MIS director or her delegate to have first-hand knowledge as to the integrity and authenticity of the electronic records nominally under her custody and control. A single lapse of password security, for example, could conceivably result in alteration of every single electronic record in the enterprise, by an interloper on the other side of the world, without any knowledge on the part of the records' custodian.

In a trial based on unprotected electronic records in the custody of the party relying upon such evidence, an opposing attorney with a strong forensic knowledge of computer security issues can be in a position to ambush and wound the credibility of routine electronic records. If the foundation testimony

is perfunctory, and the foundation witness is not properly forewarned and prepared, a blindside attack upon trustworthiness could well be effective enough to exclude the naked electronic records from evidence.

Digital Signature Through Public Key Cryptography

More recently, as dramatized by the federal government's controversial Clipper Chip initiative,[26] a number of powerful and uncrackable software schemes based on public-key cryptography[27] have been offered to bolster the security of electronic records, by providing both[28] a digital signature (for authentication and non-repudiation of electronic records) and encryption for privacy purposes.

The public key or asymmetric cryptosystem uses pairs of public and private keys which complement each other in performing encryption/decryption of a message. It is computationally unfeasible to derive the private (secret) key from knowledge of the public key.

If Alice wants to send Bob a private message, Alice uses the listed public key of Bob to encrypt a message for privacy; Bob applies his complementary private key to decipher the encrypted private message. If instead of privacy, Alice wants to digitally sign her message, Alice's message is authenticated and signed by hashing the message with a one-way hash algorithm, and then encrypting the hash with Alice's private key. Bob then applies Alice's listed public key to verify that the message was signed by Alice, and that the message was not modified subsequent to Alice's signature.

Footnotes for above:

(26) The Clipper Chip system of escrowing encryption keys with NIST and Treasury represents an effort to continue to eavesdrop on unbreakable public key cryptosystems for law enforcement and anti-terrorist purposes.

(27) RSA, Clipper/Capstone, PGP.

(28) RSA and PGP provide both encryption privacy and digital signature as "flip sides" of a single key distribution algorithms, while Clipper/Capstone uses different algorithms for encryption privacy and digital signatures. See generally, Charles R. Merrill, "Cryptography for Commerce – Beyond Clipper," *The DataLaw Report* (Sept. 1994 Clark Boardman Callaghan). The Clipper Chip system of escrowing encryption keys with NIST and Treasury represents an effort to continue to eavesdrop on unbreakable public key cryptosystems for law enforcement and anti-terrorist purposes.

a) If encryption for privacy was invoked, the security service known as privacy has been accomplished, because Bob is the only person who has Bob's private key which will decrypt the message Alice encrypted with Bob's public key;

b) If digital signature is invoked, there are three potential security services to be accomplished by a public key cryptosystem, namely "WHAT," "WHO," and

"WHEN":

1) "WHAT" represents authentication of the contents of an electronic record as of the time when the record was digitally signed with Alice's private key, namely that the contents have not been modified since it was signed;

2) "WHO" represents non-repudiation, namely that the electronic record was signed by Alice's private key, which only Alice has, with the effect that Alice cannot deny that she digitally signed the record; and

3) "WHEN" represents time-date stamping, namely verification of the time and date when the electronic record was digitally signed by Alice, using Alice's private key.

Within a public key cryptosystem functioning without security compromise, it is important to realize that the authentication (WHAT) and the non-repudiation (WHO) security services can be accomplished, but a time-date stamping (WHEN) security service is omitted. This is not the only weakness with an unenhanced public key cryptosystem.

Easing Vulnerability of Key-Based Systems With CAs

A widely recognized security weakness of any public key cryptography system is the need to reliably bind the identity of a person to that person's public key. If this binding is not reliably accomplished, then Mallet the imposter could list his own public key in a directory as the public key of Bob, the intended recipient, and then intercept and decrypt a private message intended for Bob. Alternatively, where Alice wishes to digitally sign a message, Mallet would insinuate Mallet's public key as the public key of Alice. Mallet would then use his own complementary private key to issue authenticated and signed messages in the forged name of Alice.

The secure binding of Alice's public key to the identity of Alice, and the binding of Bob's public key to the identity of Bob, requires the assistance of Trent, a trusted third-party who is sometimes referred to as a Certification Authority, or CA. Alice and Bob both present their public keys to the CA (or to two different CAs whose public keys have certificates digitally signed by a single "root" CA which is higher in a CA hierarchy) and the CA then appends a digitally-signed public key certificate to Alice's public key, certifying that "This is Alice's Public Key," and repeats the process with Bob's public key.

A further weakness of the public key system, and of any key-based system, is that if the secret, private key of the Alice is compromised for any reason, then Mallet can impersonate Alice for digital signature purposes, and private messages intended for Alice can be intercepted and read by Mallet.

Enter the Digital Notary Record Authentication System: A Keyless System of Authenticating Electronic Records

The Digital Notary Record Authentication System of Surety Inc. ("Surety") is a routine but powerful method for a corporation to authenticate the contents of

its electronic records as of a particular date and time certified by a time-date stamp, using a patented process which causes both the authentication (the WHAT) and the time stamp (the WHEN) to be factually and logically unassailable. There are no keys whatsoever, and therefore no fear of compromise of a private key and/or a public key as under the public key cryptosystem.

Here's a summary of how Digital Notary Record Authentication System works:

1. **The Customer has software in a PC[29] on its premises which is connected via the Internet[30] to a Coordinating Server (at a Surety or third party site) which runs Digital Notary Record Authentication Coordinating Server software.**
2. **Using the Digital Notary Record Authentication software on the Customer's computer, Customer hashes an electronic record ("document") into a unique 288-bit message digest ("hash digest") uniquely representing that document. Customer has the option to treat this hash digest singly, or combine (with any desired granularity) this hash digest with hash digests from other documents (an "aggregrated hash") before transmitting to a Coordinating Server (CS).**
3. **The hash digest (or aggregated hash) is transmitted to a CS, along with other identifying information. No document or other electronic record ever leaves the possession of Customer, so privacy is not compromised.**
4. **The CS software identifies the time-date when the hash digest was received, to the nearest second. It combines Customer's hash digest or aggregrated hash with all other hash digests and aggregrated hashes received from all sources during the same one-second time interval, so that there is a single "superhash" timestamped, called the "root superhash."**
5. **Every second, Surety's CS software links a time-date stamp to its root superhash for that interval, and publishes every root/time-date pair prominently in multiple online locations and also on CD-ROMS which will be periodically issued to its customers. Surety will also continue a three-year practice of publishing a weekly superhash/time-date pair in the Sunday *New York Times*.**
6. **The CS software transmits back to Customer the parameters Customer's software needs to prepare an authenticating certificate for the document (or for each document, in the case of an aggregation), namely (i) the hash digest of each document; (ii) the computation path followed when all hashes and aggregrated hashes were mathematically combined; and (iii) the time-date of the root superhash.**
7. **Customer's Digital Notary Record Authentication software issues the authenticating certificate for the document, and both document and certificate are stored in a database in Customer's computer or elsewhere, together or separately, according to Customer's preference.**
8. **When Customer subsequently needs to authenticate the time-date stamp and content of a document for itself or for a third party, Customer will locate the document and its certificate where Customer has stored. it.**
9. **Customer's Digital Notary Record Authentication software will find in the certificate the document's original hash digest and check to confirm that the newly created hash digest is identical to the original.**
10. **If the two hash digests match, it is certain that the document has not been modified since it was first hashed, although date tampering remains a possibility. If there is a match, then Digital Notary Record Authentication software uses the computation path in the document's certificate to compute the root superhash corresponding to the time-date stamp as it appears on the certificate. In parallel, the software**

retrieves either from a Coordinating Server or from a published record or CD-ROM the actual superhash value for the time-date on the certificate. If the computed superhash and the retrieved superhash are identical, there has been no date tampering. If, however, they are different, then date tampering has been detected.

Footnotes for above:

(29) The Digital Notary Record Authentication software can reside not only on a standard PC or UNIX server; it can be integrated to work with applications on any common computer platform in most networking and client/server environments. The PC platform is used only as an example and does not imply a requirement of any kind.

(30) Again, in a manner analogous to that in the foregoing footnote, the Internet is one particular medium of connectivity, but it is not a requirement. Dialup lines, leased lines, and other effective media of communication are completely compatible with the Digital Notary Record Authentication System's mode of operation.

The result is elegant and impressive. Without requiring any private or public key to be maintained, kept secure, or to be bound to any identity, the Digital Notary Record Authentication System of Surety Technologies reliably provides the authentication (the WHAT) and the time-date stamp (the WHEN) security services. Even better, the widespread contemporaneous publication of root/time-date pairs for every interval (all hashes and superhashes received during that particular second) means that no collusion is possible between Customer and Surety. The root/time-date pairs are thus non-repudiatable by Surety, which renders the WHAT-WHEN security reliable without requiring trust to be reposed in Surety.

It is immediately apparent that Digital Notary Record Authentication System is both a powerful enhancement to and a powerful substitute for the security services provided by a public key cryptosystem alone.

The Digital Notary™ Record Authentication System As a Complement to Public Key Cryptography

A certification authority running a public key cryptosystem could supply the Digital Notary Record Authentication System as an ancillary service, adding these supplemental security features to the public key service provided to the customers of the CA:

1. An independent WHEN function added to the public key WHAT-WHO service, so that it is not possible for Alice, the sender of the digitally signed message, to falsify the timedate stamp of the message.
2. A public key certificate issued by a CA must have a chronological expiration date to limit the CA's liability exposure, and to cap the length of time the CA must support certification revocation lists for revoked public keys. The Digital Notary Record Authentication System makes it possible to determine whether a key has been used within the time

period of the key's validity, without reference to any information contained in the public key itself.

3. A degree of redundant security as to authentication of the messages' contents is provided by an overlap of public key WHAT-WHO with an independent keyless Digital Notary Record Authentication System WHAT-WHEN.

The Digital Notary Record Authentication System As a New Technology for Authenticating Valid Electronic Records and Detecting Content- and Date-Tampered Illicit Records

It is also immediately apparent that the Digital Notary Record Authentication System has many applications as a standard but powerful, standalone, keyless system, particularly where a WHAT-WHEN security service is adequate without the WHO, or where it may even be desirable to eliminate the WHO feature. Here are only a few of the salient standalone WHAT-WHEN applications for which counsel may deem the Digital Notary Record Authentication System suitable:

- Record Storage. Routine authentication and time-date stamping of electronic records such as word-processing files, spreadsheets, CD-ROMs of document images, do not need the WHO security service. In fact, if WHO is eliminated from the service entirely by using the Digital Notary Record Authentication System rather than a public/private key cryptosystem, the unsettling risk of not being able to locate the private key of a departed employee is neatly sidestepped.
- Banking, Trading, and Trust Account Operations. These transactions are distinguished by their need for a strong and efficient WHEN component with fine granularity, plus an irrefutable WHAT security service component of security service. Think how much better bankers will sleep at night with the Digital Notary Record Authentication System routinely authenticating the WHAT and WHEN of billions of transactions involving trillions of dollars, in one-second batches.
- Protection of Intellectual Property. To provide irrefutable evidence of priority of invention, particularly when the invention must remain secret, the Digital Notary Record Authentication System is a method of freezing both the WHAT and the WHEN of each page of digital looseleaf laboratory notebooks. This could allow inventors to complete the transfer of all their work from sewn-page paper notebooks to PCs with increased rather than diminished time-date credibility.
- Health Care Industry. The healthcare system, paradoxically mired in paper records while confronting burgeoning electronic records, will be a fertile field for Digital Notary Record Authentication System. It can provide efficient and inexpensive authentication for the patient's personal WHAT-WHEN health care information in portable SmartCards, and also for a combination of timestamped, content-specific patient record and insurance information of great importance to all parties in malpractice cases. Not having to locate the WHO in a public key cryptosystem (private key to read encrypted information or public key to validate digitally signed information) will be a crucial advantage in many situations.
- Legal Notices. A system of reliable proof of the fact and time of filing of tax returns, transmittal of time-sensitive legal notices, and papers filed in court is an obvious "killer app" for the Digital Notary Record

Authentication System, which will be a boon to the legal profession as well as to the attorneys'clients.

Defusing the Digital Time Bomb

Finally, as if the risks and uncertainties of naked electronic records were not already sufficient to cause ulcers, a recent article by Jeff Rothenberg of the RAND Corporation in the January 1995 issue of *Scientific American* must be considered carefully. Rothenberg presents the unsettling analysis that the media on which digital electronic records are currently stored have lifetimes which are far shorter than we have come to expect and rely upon with respect to paper records! The current storage medium with the longest life - optical disk - is expected to have a physical lifetime of about 30 years, after which time binary digits will begin to degrade. Unlike the case of more robust analog recordings, the loss of even a single bit can render certain types of digital files incomprehensible. Magnetic disk, videotape, and magnetic tape are expected to lose data even faster, so that data on digital magnetic tape, for example, should be conservatively copied once a year to guarantee that none of the information is lost.

A serendipitous application for the Digital Notary Record Authentication System is its potential role as both an early-warning signal of digital file degradation in short-lived medium, and a method for automatic repair of that degradation.

If all digital records in the enterprise have been routinely processed using Surety's Digital Notary Record Authentication System, then it will be possible to detect even single-bit changes in records by re-hashing records and comparing new hash digests to original hash digests, which does not require resort to comparison with a backup copy. If a change is detected, a single backup copy will suffice to produce an automatic correction, because there will be no doubt which copy of the document is unchanged. This process of early detection and automatic correction is far more efficient than the possibilities in the absence of hashing. In the absence of Digital Notary Record Authentication System hashing, changes in a digital document cannot be detected without a bit-for-bit comparison of the entire document with a separate backup copy. Moreover, automatic correction cannot be accomplished unambiguously without reference to a second independent backup copy, because it will not be clear which of the two compared documents is the correct version.

The case for routine use of the Digital Notary Record Authentication System in your enterprise is strong even if the problem of the digital medium's degrading should eventually be solved through future technological advance. While you benefit from the advantages of electronic records with the Digital Notary Record Authentication System's provable "WHAT and WHEN" security, you will also be making progress toward defusing the digital time bomb of digital medium degradation.

Footnotes for above:

(31) Jeff Rothenberg, "Ensuring the Longevity of Digital Documents," *Scientific American* (January 1995).



Patent overviews

Method for secure timestamping of digital documents.
U.S. Patent No. 5,136,647, issued August 4, 1992.
U.S. Patent Re. 34,954, reissued May 30, 1995.

The initial patent issue covers a variety of fundamental technology and algorithmic components of digital timestamping. More specifically, the claims cover:

- The linking of timestamp requests in a sequence
- The "random-witness" method that uses the document being timestamped to pseudo-randomly choose timestamping witnesses

The subsequent reissue of the patent added some additional claims which were supported by the original specification. The additional claims cover:

- The use of a single hash value to represent a timestamp request for an "accumulation" or "collection" of digital documents
- A time-stamping process that does not explicitly require the use of a digital signature

Digital document timestamping with catenate certificate
U.S. Patent No. 5,136,646, issued August 4, 1992.

The claims of this patent cover the use of one-way hash functions to form an unalterable linked list of timestamp certificates. This makes it effectively impossible for anyone, including the timestamping service, to retrospectively fake part of the chain. In the current implementation of Surety's Digital Notary System, this linking method is how the sequence of "root hash values" are linked to form the chain of "super hash values."

Method of extending the validity of a cryptographic certificate
U.S. Patent No. 5,373,561, issued December 13, 1994.

This patent covers the use of timestamping to renew or to extend the validity of cryptographic certifications of authenticity such as timestamp certificates and digital signatures. This use enables a digitally signed record to retain its validity even if the signer's private key is later compromised, or the key's digital certificate has expired. As long as the timestamp for the record indicates that it was signed prior to the compromise of the key, or during the digital certificate's validity period, the signature is still trustworthy.

This patent also covers the parallel use of multiple hash functions in a timestamping system. Surety currently uses a combination of RSA's MD5 hash function and the NIST's Secure Hash Algorithm (SHA-1).

Method of providing digital signatures.
U.S. patent 4,309,569, issued January 5, 1982.

This patent covers the use of hash functions to build trees in order to "authenticate...an item in a list of items." This patent was originally issued to Stanford University with Ralph Merkle as the inventor. It was subsequently licensed exclusively to Public Key Partners (PKP) in 1993. In March 1994, Surety signed a license agreement with PKP granting Surety an exclusive sub-license for the use of this patent within the domain of use of digital time-stamping.

Digital document authentication system.
U.S. Patent No. 5,781,629, issued July 14, 1998.

This patent covers Surety's current method for assigning SureID numbers to documents. A SureID number is a short, unique, cryptographically secure identifier produced for any digital document, record, or message that is notarized by the Surety Digital Notary Service. The patent also covers several extensions to the use of SureID numbers that Surety has not yet implemented, and provides additional claim coverage to protect Surety's timestamping methods.

Foreign patent applications

Patents have been issued and/or patent applications have been filed in Canada, Japan, New Zealand, China, South Korea, Singapore, Mexico, Brazil, Argentina,

Belgium, Germany, Switzerland, Spain, France, the United Kingdom, Italy, the Netherlands, Sweden, and Australia.